Detecting Selfish nodes in MANET using Record-Trust based- Detection with Collaborative Watchdog

P. Prasath
P.G Scholar,
Department of Computer Science & Engineering,
University College of Engineering,Trichy.

***Abstract* — In the last decade, mobile ad hoc networks (MANETs) have emerged as a major next generation wireless networking technology. Security has become one of the major concerns in MANETs. One of the different kinds of misbehaviour a node may exhibit is selfishness. A selfish node wants to preserve own resources while using the services of others and consuming their resources.The overall network performance could be seriously affected. The purpose of this project is to develop Intrusion Detection System and gives a deep understanding of some sophisticated techniques for intrusion detection. One way of preventing selfishness in a MANET is a detection and exclusion mechanism. In this paper selfish nodes are detected using Record- and Trust-Based Detection (RTBD) Technique with Collaborative Watchdog. Collaborative approach is based on the diffusion of local selfish nodes awareness when a contact occurs, so that information about selfish nodes is quickly propagated. The main reason for using trust in this analysis is to accelerate the detection of misbehaving nodes.**

Keywords*— *MANETs, Selfish nodes, Packet delivery ratio, Route discovery

1 INTRODUCTION

1.1 What is selfish node?

Mobile ad hoc network (MANET) is a wireless network among mobile devices. It is a self-configuring system of mobile nodes connected by wireless links, which contains a network area with nodes. This network is relatively a new communication paradigm, which contains a group of mobile devices communicating through a wireless medium. Each mobile node in MANET requires the help of other nodes to forward the packets. The nodes are expected to wait for a pre-defined time interval between successive transmissions. But a mobile node may misbehave due to network congestion and selfishness.
Node misbehaviour due to selfish or malicious reasons or faulty nodes can significantly reduce the performance of MANETs. Node misbehaviour means deviation from the original routing and forwarding. The source node can relay packets to the destination node through other nodes in MANET. The selfish nodes do not participate in the routing process, which intentionally delay and drop the packet. These misbehaviours of the selfish nodes will impact the efficiency, reliability, and the fairness. A selfish node does not perform the process related to packet forwarding function for data packets unrelated to itself. The selfish node utilizes its limited resources only for its own purpose because of the energy and storage constraints for each node in the MANET. It aims to save its resources to the maximum, so this type of misbehaving node discards all incoming packets except those which are destined to it. The selfish nodes neglect to share their resources, such as battery power, CPU time, and memory space to other nodes in MANET.

1.2 The features of selfish nodes

- Non-participation in routing.
- No transmission or reply to HELLO messages.
- Intentional postponement of route request (RREQ) packets.
- Data packet dropping.

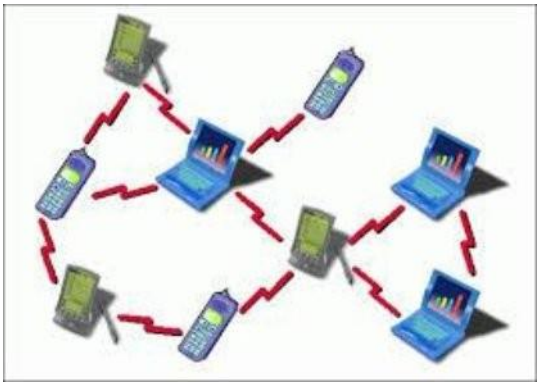

Fig.1.basic MANET architecture

2 RELATED WORK

This section deals with the existing solutions for handling and detecting the nodal misbehaviour in MANET.
M.Hollick et al.[27] discussed the influence of node misbehaviour on the routing process. In particular, they derived a classification for misbehaving nodes and extend an analytical model of the route acquisition process executed by the Ad hoc On-demand Distance Vector (AODV) routing protocol to cover different

classes of misbehaviour. The validation of the behaviour model, and the clarification of the impact misbehaving nodes impose onto the routing process, is completed using an experimental analysis. J.Hortaleno et al.evaluate the usefulness of watchdog modules for intrusion detection. Contributions of their work are threefold. First, the component is designed to be protocol independent, thus compatible with any different types of ad hoc routing protocols. Second, it encompasses high detection coverage with low detection latency. Third, the previous properties are guaranteed while minimizing the number of generated false positives and negatives the provided design is implemented and evaluated. Results show that a set of trade-offs must be adopted in order to obtain an acceptable balance between the coverage and detection latency of the watchdog and the resources required from devices. F.Kargl et al.[3] focused on the detection phase and present different kinds of sensors that can be used to find selfish nodes. They present a simulation results that show the negative effects which selfish nodes cause in MANET. In the related work section they analysed some of the detection mechanisms. They are developed a mechanism called activity-based overhearing, iterative probing, and unambiguous probing.

Simulation-based analysis of these mechanisms shows that they are highly effective and can reliably detect a multitude of selfish behaviours. Q. Li, S. Zhu, and G. Cao[4] proposed a Social Selfishness Aware Routing (SSAR) algorithm to allow user selfishness and provide better routing performance in an efficient way. To select a forwarding node, SSAR considers both users' willingness to forward and their contact opportunity, resulting in a better forwarding strategy than purely contact-based approaches. Moreover, SSAR formulates the data forwarding process as a Multiple Knapsack Problem with Assignment Restrictions (MKPAR) to satisfy user demands for selfishness and performance. Trace- driven simulations show that SSAR allows users to maintain selfishness and achieves better routing performance with low transmission cost.Y.Li et al.[5] are investigated how the selfish behaviours of nodes affect the performance of DTN multicast and consider two typical multicast relaying schemes, namely, two-hop relaying and epidemic relaying, and study their performance in terms of average message transmission delay and transmission cost. Specifically, they modelled message delivery process under selfish behaviours by a 3-D continuous time Markov chain; under this model, they derived closed-form formulas for the message transmission delay and cost and evaluate the accuracy of the Markov chain model by comparing the theoretical results with the simulation results obtained by simulating the message dissemination under both two-hop and epidemic relaying with different network sizes and mobility models. They showed that different selfish behaviours may have different impacts on different performance metrics. In addition, selfish behaviours influence epidemic relaying more than two-hop relaying. Furthermore, they explained performance of multicast with selfish nodes depends on the multicast group size. Y.Zhang et al.[6] addressed the problem of identifying and isolating misbehaving nodes that refuse to forward packets in multi-hop ad hoc networks and developed a comprehensive system called Audit-based Misbehaviour Detection (AMD) that effectively and efficiently isolates both continuous and selective packet droppers. The AMD system integrates reputation management, trustworthy route discovery, and identification of misbehaving nodes based on behavioural audits. Compared to previous methods, AMD evaluates node behaviour on a per-packet basis, without employing energy- expensive overhearing techniques or intensive acknowledgment schemes. Moreover, AMD can detect selective dropping attacks even if end-to-end traffic is encrypted and can be applied to multi-channel networks or networks consisting of nodes with directional antennas. They simulated that AMD successfully avoids misbehaving nodes, even when a large portion of the network refuses to forward packets.Ciobanu.R et al.[19] developed a novel collaborative content and context-based selfish node detection algorithm and an incentive mechanism which aim to reduce the issues of selfish nodes in an opportunistic network. Local information may not be sufficient to reach an informed decision, nodes running in algorithm collaborate through gossiping, for the final goal of detecting selfish nodes, later on to punish and avoid them and compare their approach to an algorithm entitled IRONMAN and show that it behaves better in terms of network performance and detection accuracy.Wang Xing-Wei et al.[8] allowed nodes to freely express their subjective forwarding willing the detection mechanism is implemented punishing nodes which have a higher selfish degree than given threshold or lie about its information, the Stimulation mechanism is implemented. Stimulation results show that the detection mechanism and stimulation mechanism not only can discover appropriate routing, but also can stimulate selfish nodes to actively cooperate when the degree of nodes selfishness is excessive. Bo Chen et al. proposed Incentive Detection Mechanism (IDM) for cooperation of nodes selfish behaviour. This mechanism consists of two parts which are detection module based on retransmission numbers and punishment module. The detection module determines if there is a selfish behaviour in the networks by collecting average retransmission numbers of nodes itselves and finding the maximum value of average retransmission numbers, then comparing the difference of average retransmission numbers and maximum value with the set threshold value; The punishment module change the strategy of selfish nodes for cooperation with normal nodes so that the network performance can improve. The experimental results show that the IDM can improve the detecting rate and lower the false detecting rate in appropriately selected detection mechanism parameters, and every node link can obtain a relatively fair throughput to improve the performance of overall networks. Yi-an Huang and Wenke Lee reported in developing intrusion detection (ID) capabilities for MANET. Building on prior work on anomaly detection,

they investigated how to improve the anomaly detection approach to provide more details on attack types and sources. For several well-known attacks, they applied a simple rule to identify the attack type when an anomaly is reported. In some cases, these rules can also help identify the attackers. They addressed the run-time resource constraint problem using a cluster based detection scheme where periodically a node is elected as the ID agent for a cluster. Compared with the scheme where each node is its own ID agent, this scheme is much more efficient while maintaining the same level of effectiveness and conducted extensive experiments using the ns-2 and MobiEmu environments to validate our research. Sorav Bansal and Mary Baker developed OCEAN technique is to avoid trust- management machinery and see how far we can get simply by using direct first-hand observations of other nodes' behaviour. OCEAN can do as well as, or even better than, schemes requiring second-hand reputation exchanges. This encouraging result could possibly help obviate solutions requiring trust-management for some contexts. Yang Qin et al. showed that MANETs are still vulnerable under passive statistical traffic analysis attacks. To demonstrate how to discover the communication patterns without decrypting the captured packets, they presented a novel statistical traffic pattern discovery system (STARS). STARS works passively to perform traffic analysis based on statistical characteristics of captured raw traffic. STARS is capable of discovering the sources, the destinations, and the end-to- end communication relations.

3 SYSTEM MODEL

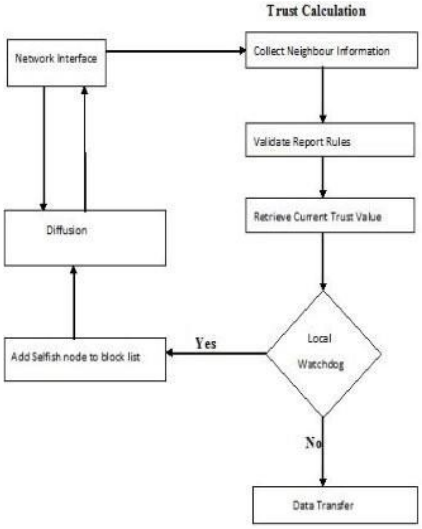

Fig.2.system architecture

4 PROPOSED SYSTEM DESCRIPTION

The main objective of the proposed work is to detect the selfish node in MANET using the Record- and Trust-Based Detection (RTBD) technique with Collaborative Watchdog. The proposed method consists of a packet dropping detection scheme and a selfish node mitigation scheme. The selfish node is required to generate a trust report during each neighbour, which reports its previous communication reports to the neighbouring node. Based on that report, the neighbouring node detects if the selfish node has dropped packets. The neighbouring node gathers the trust report to detect misreporting and then it finds out which node has dropped packets. A selfish node may report a false record to hide the dropping from being detected.

4.1 Route discovery

Route discovery allows any node in a MANET to dynamically discover a route to any node in MANET. The initial step of route discovery is to create the number of nodes with the indicated position. By sending the RREQ packet, the route is discovered between the source node and the destination node. A node initiating a route discovery broadcasts a RREQ message, which may be received by those nodes within wireless transmission range. If the route discovery is successful, the initiating node receives a route reply message listing a sequence of network hops.

4.2 Selfish node detection

The MANET is modelled and the nodes in the network are deployed according to the architectural model. Numerous nodes will be participating in the MANET for forwarding and transmitting the data packets between the source and destination. All the nodes in MANET perform the routing function as mandatory and they must forward traffic, which other nodes sent to it. Among all the nodes, some of the nodes will behave selfishly; these types of nodes are called selfish nodes. Any node in MANET may act selfishly, which means using its limited resources only for its own profit, since each node in a network has the resource constraints such as storage and battery limitations. This type of nodes likes to enjoy the profits provided by the resources of other nodes in the network. But it should not make its own resource accessible to others.

These nodes intent to get the greatest benefits from the network while trying to preserve their own resources.

The behaviours of the selfish nodes are shown below:

- Do not forward RREQ messages. This type of nodes does not forward the RREQ messages in MANET. It drops these packets to avoid being the route member for others.
- Do not forward data messages. This kind of selfish nodes will forward the messages, but it will not relay data messages and drop them. This misbehaviour will impact the performance of MANET.
- Delayed forwarding RREQ messages. This kind of selfish nodes forwards the messages with a delay near the upper limit of timeout.
- Do not forward RREP messages. If this kind of selfish node exists in MANET, it will drop all RREP messages received by these nodes.

4.3 Record- and trust-based detection technique

In this framework, every node maintains a global trust state for all selfishly behaving nodes in the network. The trust state is maintained in the form of a trust table. A trust table contains two fields, namely n-id (node id) and t-Val (trust

value). When a node receives a new trust certificate, the trust state of a node is updated. The certificate is evaluated by verifying the response from every neighbour in the group. The impact of trust certificate in the final trust value of a suspected node depends on the trust state of the node.
For updating the trust value of a node, the following function is used

$$(1-T_{new}) = a(1-T_{old}) + b(1-T_C)-F$$

Where a and b represent the weightage corresponding to the old trust and new trust values of the node. F is the trust replenishment factor over time. B depends on three factors a1, a2, and a3. The parameter b can be expressed

$$b = a1 \times a2 \times a3$$ The

parameter $a1$ is

$$a1 = \sum_{max} W_i T_i / W_n$$

Where Wi and Ti depicts the weightage and trust value, respectively, belonging to the majority group of the neighbours of the accused node. Wn is a factor that depends on the size of the network. a2 represents the weightage given to the new trust value, and the value of a3 is obtained using

$$a3 = \{ 1 \text{ if } k =1, 1 \text{ if } k > 1$$

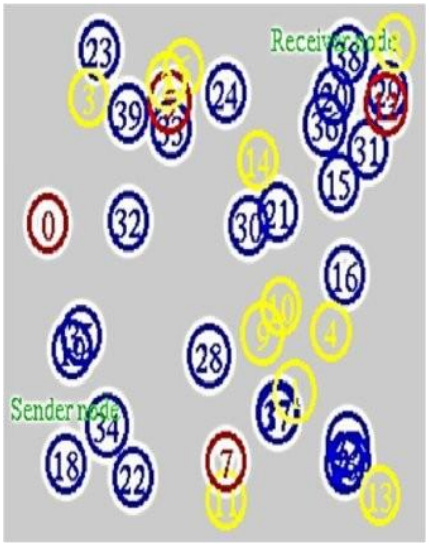

Fig.3.manet with selfish nodes

5 PERFORMANCE ANALYSIS

This section presents the results of the proposed method, namely RTBD technique with Collaborative Watchdog. The initial step involves the detection of the verified block listed nodes among the mobile nodes in MANET. The difference between the normal nodes and the verified block listed nodes are shown by different colour. The selfish nodes among the verified block listed nodes are detected in the second step. The detected selfish nodes are highlighted by red colour. Packet delivery ratio (PDR) is the ratio between the number of packets transmitted by a traffic source and the number of packets received by a traffic sink. It measures the loss rate as seen by transport protocols, and it characterizes both the correctness and efficiency of ad hoc routing protocols. The implication of not forwarding the packets or dropping the packets in MANET leads to a serious problem. So, this analysis addresses this event and gives higher priority for packet dropping in MANET. The packet drop rate is observed in the selfish node detection method, namely RTBD. The comparative analysis is performed with respect to the number of nodes. Selfish node detection is an important concern in MANET, so this study fully concentrates the detection of selfish nodes in an efficient manner by using RTBD with Collaborative technique. The detection rate of the selfish behaviour is observed by using the RTBD method. Compared to the existing method, the proposed RTBD method significantly increases the detection ratio.

6 CONCLUSION

The misbehaviour of selfish nodes is a major problem in MANET. The selfish nodes do not participate in the routing process, which intentionally delay and drop the packet. These misbehaviours of the selfish nodes will impact the efficiency, reliability, and fairness. The selfish node utilizes the resources for its own purpose, and it neglects to share the resources to other nodes. So, it is important to detect the selfish nodes in MANET. This study proposes a new technique, namely RTBD with Collaborative Watchdog, to detect the selfish nodes in an efficient manner. The suggested RTBD method is an effective method, which enhances the performance of MANET. It significantly improves the performance metrics such as PDR and detection ratio. Moreover, it diminishes the overhead, latency, and packet dropping ratio. Compared to the existing method, the proposed method competently detects the selfish nodes in MANET.

REFERENCES

[1] Enrique Hernandez-Orallo, Manuel David Serrat Olmos, Juan-Carlos Cano, Carlos T. Calafate, and Pietro Manzoni, 'CoCoWa: A Collaborative Contact-Based Watchdog for Detecting Selfish Nodes',IEEE Transactions on Mobile Computing, Vol. 14, No. 6.2015

[2] Y.Hu, B. Johnson and A. Perrig, "SEAD: Secure Efficient Distance Vector Routing for Mobile Wireless Ad Hoc Networks", International Journal of Ad hoc Networks, Vol.1, pp 175-192, 2003.

[3] F. Kargl, A. Klenk, S. Schlott, and M. Weber , 'Advanced detection of selfish or malicious nodes in ad hoc networks', Proceeding International Conference on Security Ad-Hoc Sensor Networks pp 152-165.2004

[4] Q. Li, S. Zhu, and G. Cao, 'Routing in socially selfish delay tolerant networks', IEEE Conference on Computer Communication, pp. 857– 865.2010

[5] Y. Li, G. Su, D. Wu, D. Jin, L. Su, and L. Zeng, 'The impact of node selfishness on multicasting in delay tolerant networks', IEEETransaction on Vehicle Technology, Vol. 60, no. 5, pp. 2224–2238,2014.

[6] Zhang, L. Lazos, and W. Kozma, 'AMD: Audit-based misbehaviour detection in wireless ad hoc networks', IEEE Transaction on Mobile Computing, Vol. PP, no. 99.2012.
[7] E. Hern_andez-Orallo, M. D. Serrat, J.-C. Cano, C. M. T. Calafate, and P. Manzoni, 'Improving selfish node detection in MANETs using a collaborative watchdog', IEEE Communication Letters, Vol. 16, no. 5, pp. 642–645,2012.
[8] Wang Xing-Wei and Qu da-Peng , 'Selfish nodes detection mechanism and stimulation mechanism over mobile peer-to-peer networks', IEEE Conference on Industrial Electronics and Applications, pp.1030- 1034,2012.
[9] E. Hernandez-Orallo, M. D. Serrat Olmos, J.-C. Cano, C. T. Calafate, and P. Manzoni, 'Evaluation of collaborative selfish node detection in MANETS and DTNs', International Conference on Wireless Mobile System, pp. 159-166,2012.
[10] B. Sun, K. Wu and U.W. Pooch, "Routing Anomaly Detections in Mobile Ad Hoc Networks", Proc. IEEE International Conference on Computer Communication and Networks ICCCN, 2003.
[11] J. Kong, X. Hong and M. Gerla, 'A new set of passive routing attacks in Mobile ad hoc networks', IEEE Military Communication Conference MILCOM,2003.
[12] A.Hijazi and N.Nasser, "Using Mobile Agent for Intrusion Detection in Wireless Ad-Hoc Networks", Proc. IEEE Wireless Communication and Networking Conference WCNC, March 2005.
[13] B.Smith, "An Examination of Intrusion Detection Architecture for Wireless Ad-Hoc Networks", Proc. National Colloquium for Information System Security Education, May 2001.
[14] K.Sanzgiri and M.Belding-Royer, "A Secure Routing Protocol for Ad Hoc networks", Proc. IEEE International Conference on Network Protocol (ICNP' 02), 2002
[15] H.Jiang and H.Wang, "Markov Chain Based Anomaly Detection for Wireless Ad-Hoc Distribution Power Communication Networks", Proc. IEEE Power Engineering Conference, 2005.
[16] Sengathir, J and Manoharan, R, 'A split half reliability coefficient basedmathematical model for mitigating selfish nodes in MANETs' IEEE Conference on Advance Computing, pp. 262-267,2013.
[17] C Jae-Ho, S Kyu-Sun, L SangKeun, W Kun-Lung, 'Handling selfishness in replica allocation over a mobile ad hoc network', IEEE Transactions on Mobile Computing 11, 278–291,2012.
[18] PB Velloso, RP Laufer, D d O Cunha, 'Trust management in mobile ad hoc networks using a scalable maturity-based model', IEEE Transaction on Network Service Management,2010.
[19] R-I Ciobanu, C Dobre, M Dascalu, S Trausan-Matu, V Cristea, 'Collaborative selfish node detection with an incentive mechanism for opportunisticnetworks', International Symposium on Integrated Network Management pp. 1161–1166,2013
[20] P. Yi, Y. Jiang, Y. Zhong and S. Zhang, 'Distributed Intrusion Detection for Mobile Ad Hoc Networks', IEEE Application and Internet Workshop,2005.
[21] B. Sun, L. Osborne, Y. Xiao, and S. Guizani, "Intrusion Detection Techniques in Mobile Ad Hoc and Wireless Sensor Networks," IEEE Wireless Communications Magazine, special issue on Security in Wireless Mobile Ad Hoc and Sensor Networks, Vol.14, No.5, pp. 56- 63, Oct.2007.
[22] Y.Hu, A.Perrig and B.Johnson, "A Secure On Demand Routing Protocolfor Ad Hoc networks", Proc. ACM/ IEEE International Conference onMobile Computing (MobiCom), Atlanta, Georgia, USA, pp 23-28, Sep.2002.
[23] T. He, H. Wang and K.W. Lee, "Traffic analysis in anonyms MANETs",Proc. IEEE Military Communication Conference MILCOM, November 2008.
[24] O.F. Gonzalez-Duque, M. Howarth and G. Pavlou, "Detection of Packet Forwarding Misbehaviour in Mobile Ad hoc Networks", Proc. International Conference on Wired/Wireless Internet Communications (WWIC2007), pp 302-314, Portugal, June 2007.
[25] Sengathir, J and Manoharan, R, 'A split half reliability coefficient based mathematical model for mitigating selfish nodes in MANETs' IEEE Conference on Advance Computing, pp. 262-267,2013.
[26] C Jae-Ho, S Kyu-Sun, L SangKeun, W Kun-Lung, 'Handling selfishness in replica allocation over a mobile ad hoc network', IEEE Transactions on Mobile Computing 11, 278–291,2012.
[27] M. Hollick, J. Schmitt, C. Seipl, and R. Steinmetz, "On the effect ofnode misbehavior in ad hoc networks," in Proc. IEEE Int. Conf. Commun., 2004, pp. 3759–3763.
[28] PB Velloso, RP Laufer, D d O Cunha, 'Trust management in mobile ad hoc networks using a scalable maturity-based model', IEEE Transaction on Network Service Management,2010.
[29] B. Sun, L. Osborne, Y. Xiao, and S. Guizani, "Intrusion Detection Techniques in Mobile Ad Hoc and Wireless Sensor Networks," IEEE Wireless Communications Magazine, special issue on Security in Wireless Mobile Ad Hoc and Sensor Networks, Vol.14, No.5, pp. 56- 63, Oct.2007.